View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Asia University Academic Repositories

論説

EU個人データ保護法における十分性審査と日本の対応

加藤隆之

一　ＧＤＰＲと十分性審査

㈠　ＧＤＰＲの制定経緯

二〇一二年一月、欧州委員会は、ＥＵのデータ保護制度の包括的な改革案を提唱した(1)。この改革案において、欧州委員会は、従来のデータ保護指令(2)に代わって加盟国を直接義務づける規則とすること（General Data Protection Regulation, ＧＤＰＲ）、及び、主に刑事法執行機関による取扱いにおける個人データの保護を対象とした、新たなデータ保護指令（新指令）を制定することを求めた(3)。

ＧＤＰＲの目的としては、デジタル時代における市民の基本的権利を強化すること、「デジタル単一市場」の中で企業に対するルールを簡素化することによって取引を促進すること、単一の法を制定することによって加盟国間で差異のある法制度及び費用のかかる行政上の負担を減らすことなどがあげられている。

また、新指令の目的は、犯罪の被害者、証人及び被疑者の個人データが適切に保護され、犯罪やテロへの戦いに際して、越境的協力を促進することとされている。

そして、欧州委員会は、二〇一五年一二月から、欧州議会及び理事会と最終的な文書の合意に向けた交渉に入った。二〇一六年四月には、理事会と欧州議会とが続けて、ＧＤＰＲ(4)及び二つの新指令(5)を採択した。同年五月四日には、すべての公式言語で表わされたこれらのルールの条文がＥＵ公式ジャーナル（EU Official journal）で

公表された。ＧＤＰＲは二〇一六年五月二四日に発効し、二〇一八年五月二五日から施行される。他方、新指令は、二〇一六年五月五日に発効し、ＥＵ加盟国は、二〇一八年五月六日までに、それを国内法化しなければならないことになっている。

本稿の目的は、より一層の個人情報保護を図ったＧＤＰＲと日本が今後いかに向き合っていくべきかについて検討することにある（それゆえ、上記新指令については割愛する）。つまり、データ保護法の制定以来、日本は欧州から個人データ保護制度において十分なレベルにあると認定されていないが、それはなぜなのか、また、日本は今後いかにＥＵと対峙すべきなのかについて考えてみたい。

また、本稿では、ＥＵの十分性審査を中心とした個人データ保護法におけるＥＵと日本との関係の全体像、そして、それに対する私見を素描することを目的としているため、個々の細部にわたる論点に対して論じ切れていない部分がある。これらについては、向後、順次明らかにしていきたいと思う。

(二) ＧＤＰＲの十分性審査の概要

(a) データ保護指令における十分性審査

ＥＵデータ保護指令二五条一では、原則的に、個人データが第三国へ移転される場合には、当該第三国が十分な保護レベルを有していなければならない旨の規定を加盟国がおかなければならないと定めている。つまり、欧州経済領域（the EUropean Economic Area, ＥＥＡ）から個人データを移転する場合には、移転先の国がこの十分性審査をクリアーしていることが求められている。

そして、同条の二では、十分性の審査は、データ移転に関連するあらゆる状況に照らして行うとし、その際に

は、とりわけ、データの性質、求められている取扱作業の目的及び期間、データの発生地及び最終目的地、また、当該第三国で施行されている一般法及び個別法の法規範などを考慮すべきとしている。

さらに、二九条作業部会（**Article 29 Working Party**）は[6]、**WP** 一二において、この十分性審査の意味をより明確化した[7]。同文書の第一章㈠では、第三国の法制度について、その「内容」（**content**）と「執行」（**enforcement**）の双方の側面から審査する旨を強調している。これに従い、十分性審査について検討する際、実体的な内容の保護レベルに関する事項と、それを実現するための執行制度に関する事項とを分けて考えることが有益である。

(b)　GBPRにおける十分性審査

GDPRでは、基本的に、こうしたデータ保護指令の基本的なスタンスを維持している。つまり、同規則四一条一では、第三国へのデータ移転は、原則的に当該第三国が十分なデータ保護のレベルを有する場合であることとし、その十分性判断は欧州委員会が決定するとしている。

そして、GDPR四五条二では、その審査において、考慮すべき具体的な要素について明示している。データ保護指令では明示されていなかったものの、その要素として次の事項があげられていることが特徴的である。

①　公安、国防、国家の安全及び刑事法並びに個人データへの公的機関のアクセスに関する法律

②　個人データを再移転する場合、その再移転先の第三国や機関におけるデータ保護水準

③　独立した監督機関の設置

まず、①は、後にみる***Schrems***判決[8]を考慮したものと考えられる。②は、データ保護指令のもとで行われていた審査の欠陥として指摘されていた[9]重大な部分を穴埋めしたものである。③について、データ保護指令では、独

立した監督機関の存在が要件として明示的に求められていなかったが、これを明文化している。

㈢　十分性決定の認定国

データ保護指令下において、欧州から十分なデータ保護制度を有しているとの評価を受けている一二の国や地域は、二〇一六年一二月現在で、次の通りである（十分性決定を受けた順[10]）。

「スイス、カナダ（営利組織）、アルゼンチン、ガーンジー、マン島、ジャージー、フェロー諸島、アンドラ、イスラエル、ウルグアイ、ニュージーランド、アメリカ合衆国のプライバシー・シールド」

このうち、ガーンジー、マン島、ジャージーの三つの地域は、イギリス王室属領である。また、フェロー諸島は、デンマークの自治領である。こうした地域では、その属している国との関係が深いわけであるから、その法制度を模倣する傾向にある。もっとも、二〇一六年六月に、イギリスがＥＵ離脱を国民投票で決定したため、今後、仮にそのイギリスがＥＥＡからも脱退ということになると、その王室属領である三地域が、ＥＵの十分性基準をフォローするのか疑わしくなるかも知れない。ともあれ、この四地域を除くと、十分性認証を受けた国はわずか七か国であるが、そのうち、アンドラはスペインとフランスの国境にある非常に小さな国である。

よって、ＥＵが十分性を認めた本質的に意味のある第三国は、アルゼンチン、カナダ（営利組織）、イスラエル、ニュージーランド、スイス、アメリカ合衆国、ウルグアイという、その数わずか七か国に過ぎないということになる。ところが、さらに、このうちのカナダとアメリカ合衆国は、国全体としての十分性が認定されたわけではない。また、残りの国でＥＵとの貿易が盛んな国はスイスのみであり、そのスイスは、ＥＵに加盟していないも

のの、ヨーロッパ大陸の中心に位置するため、その法体系は、大陸法系のEU加盟国に近いものと推測されよう。結局、EUから地理的にも離れて、データ保護の十分性を全面的に認められた国は、アルゼンチン、イスラエル、ニュージーランド、ウルグアイのわずか四か国しか存在しないということになる。しかも、私の個人的主観であり、失礼かもしれないが、アルゼンチンやウルグアイ（いずれもスペインの植民地であった）という南米の国々が、日本よりも高度な個人情報保護が図られているというのであれば、少なくとも実態としては、にわかに信じがたいものがある。(11)

欧州データ保護指令は、一九九五年一〇月に成立していることから、二〇年以上経過していることになる。この二〇年間を超える期間で、形式的にみて一二の国や地域が、また、実質的にみて六（若しくは四）つの国が、十分性ありと認定されたということになる。(12)これは、果たして、制度として成功したといえるのだろうか。

(4) *Schrems* 判決の衝撃

(a) 事実の経緯

EUは、かつて、最大の貿易相手国であるアメリカ合衆国とは、EU市民のデータ保護を目的として、セーフ・ハーバー（Safe Harbour）協定を締結し、欧州委員会は、この協定が十分な保護レベルにあると判断していた。(13)ところが、オーストリア国籍の大学院生Schrems氏が、アメリカ合衆国を揺るがしたPRISM事件を契機として、フェイスブックにおける自らの個人データがセーフ・ハーバーの仕組みの下、ダブリンに置かれている支店（ヨーロッパ本社）からアメリカ合衆国の本社に送られ、アメリカ国家安全保障局（US National Security Agency）に情報提供されているという事実を知ったため、アイルランドのデータ保護コミッショナーに調査す

るよう申し立てた。

しかし、同コミッショナーは、同申立てが取るに足らない訴権濫用の（frivolous and vexatious）[14]ものであること、また、アイルランドのデータ保護法では、EU法（欧州委員会の判断もその一部）に拘束されることを理由に、同調査を行わないと決定した。そこで、その決定を不服としたSchrems氏は、アイルランド高等裁判所に提訴した。

同高等裁判所は、二〇一四年に、同コミッショナーが本件調査を開始すべきか、それとも、アメリカ合衆国の個人データ保護のレベルが十分であるとした欧州委員会の決定に拘束されるべきかについての判断を求めて、欧州司法裁判所（the Court of Justice of the European Union）に先決裁定を求めることを決定した[15]。

そして、二〇一五年一〇月六日、欧州司法裁判所は、欧州委員会の決定（decision）があっても、コミッショナーの調査権限が制約されるわけではないと判断し、続いて、アメリカ政府が機微情報を含めた個人データにアクセス可能となっており、その場合の法的救済手段を欠いていることなどを根拠として、セーフ・ハーバー協定の十分性を認めた欧州委員会の決定を無効[16]と判示した[17]。

その後、アメリカ合衆国では、法改正や新たな法律の制定などを行うと同時に、欧州委員会との間で、セーフ・ハーバーに代えたプライバシー・シールド（Privacy Shield）という新たな協定の策定について協議を続け、二〇一六年二月にはその合意にこぎつけた[18]。そして、二〇一六年七月一二日、欧州委員会は、この新協定が十分な保護レベルにあると判断した[19]。

このように、当事国であるアメリカ合衆国に与えた*Schrems*判決の影響は、非常に大きかった。しかし、同時に、EUにとっても大きな痛手を伴うものであった。なぜなら、この訴訟や判決によって、EUの十分性審査が

決して盤石なものではなく、むしろ、欠陥を有しているのではないかということが明らかとされたからである。また、EUと最大の貿易相手国であるアメリカ合衆国との協定であったことも、関係者に大きなショックを与える要因となった。

(b)　代替的手段Ⅰ―BCRs及びSCCs

*Schrems*判決後、二九条作業部会は、セーフ・ハーバーを利用していた企業に対し、これに代わる手段として拘束的企業ルール（Binding Corporate Rules、BCRs）や標準契約条項データ保護制度（Standard Contractual Clauses、SCCs）を代替手段として示唆した(20)。

しかし、国家の安全にかかわる事項を前にしては、こうした手段が無力なのではないかという疑念が生じる。なぜなら、これらの手段は、その法的基礎を契約においており、その中でいかに高度な個人情報保護措置を講じられていたとしても、国家の安全に関する立法（security law, intelligence law）に基づく個人情報の収集に対して、公権力の行使を排除することはできないからである。それゆえ、これらのツールを利用したとしても、常に、EU市民のデータが送られた第三国における安全保障に関する立法が、EUの十分性基準を充足できるのかという問題が立ちはだかることになる。

このような懸念は、多くの個人データ保護の専門家が享有するものであると思われるが、それはSchrems氏も例外ではなかった。二〇一五年の*Schrems*判決後、Schrems氏は、アイルランドのデータ保護コミッショナーに対し、それまで申し立てていた苦情を修正する形で、SCCsが十分な保護レベルにないと申し立てた。フェイスブックなど多くのインターネット企業が、同判決後、アメリカ合衆国への個人データ移転に関しては、SCCs

依拠していたからである。

そして、二〇一六年五月には、同コミッショナーは、このSchrems氏の主張を認め、SCCsがEU基本権憲章（the European Union Charter of Fundamental Rights）四七条に反するという仮決定を行った。さらに、同コミッショナーは、SCCsに対する欧州委員会の決定の妥当性に関する宣言、及び、欧州司法裁判所にこの問題に関する先決裁定のため付託することについての判断を求めて、アイルランド高等裁判所において法的手続を開始した[21]。

(c)　代替的手段Ⅱ―同意

なお、同意をセーフ・ハーバーの代替手段とすることも考えられるが、同意については、二九条作業部会が、二〇一一年に出した文書において、継続的又は組織的なデータ移転の場合、それが有効なツール足り得ないことを示唆しており[22]、学説上もこれを支持する見解が多いようである[23]。

もっとも、GDPRでは、この立場を微妙に変化させているように思われる。四九条一では、四五条(3)による十分性決定、若しくは、BCRsなどの四六条による適切な安全措置を欠く場合に、個人データの第三国移転が許される場合について定められており、その(a)では、データ主体の同意がある場合をあげている。

具体的には、十分性の決定及び適切な安全対策が存在しないために、データ主体に関する当該移転によって生じ得るリスクについての情報が提供された後、データ主体がその提案された移転に明示的に同意した場合に、越境的データ移転が許されるという。

確かに、十分性の決定、若しくは、四六条による適切な安全措置をとることが第一に求められているが、例外的にせよ、同意による継続的・組織的越境データ移転を肯定している点では、前述の二九条作業部会の見解と齟

齟齬があるように思われる。

二　十分性審査の問題点

㈠　実体的内容に関する十分性（substantive content adequacy）

十分性審査の基準は、ＧＤＰＲ四五条でその具体的内容が示されている。しかし、これらは依然として、第三国にとって明瞭であるとはいいがたい。まず、実体的内容に関する十分性審査についていえば、第三保護法がいかなる程度高度な保障をデータ主体に与えていれば、十分な保護を与えていると解されるのか明らかではない。

(a)　ＧＤＰＲと日本の改正個人情報保護法

この点をあぶりだすために、ＧＤＰＲと改正された日本の個人情報保護法との間において、主要と思われる実体的内容に関する齟齬についていくつかみてみたい。

①　改正個人情報保護法一五条二項では、利用目的の変更について、変更前の利用目的と関連性を有すると合理的に認められる範囲において許容することとしたが、ＧＤＰＲではこのような規定が存在せず、五条一(b)では、収集時の目的と相容れない更なる取扱いを禁じている。

②　ＧＤＰＲ一七条は、**Google Spain** 判決を受けて[24]、いわゆる忘れられる権利（**right to be forgotten**）に関する定めをおいているが、改正個人情報保護法は、この権利を保障していない。

③　ＧＤＰＲ三三条、三四条では、個人データの取扱いについて違反行為があった場合に、それを監督機関やデータ主体に通知（**notification of personal data breach**）する義務について定めをおいているが、少なくとも一般法である改正個人情報保護法では、このような定めは存在しない[25]。

④　ＧＤＰＲでは、継続的な第三国への個人データ移転について、同意に基づいて行うことを原則的には認めていないにもかかわらず（四九条一(a)を参照）、改正個人情報保護法二四条ではこれを認めている。

以上のような比較的明白な差異に比して、現時点では必ずしも判然としていないように思われるが、個人情報の定義・解釈がＧＤＰＲと個人情報保護法とでは一致しない可能性がある[26]。この定義の該当性は、義務規定の適用の有無を決するのであるから、実は、この点が重大な争点となるように思われる。

こうした齟齬が、ＥＵの十分性審査に影響するのかについては未知数であるが、改正個人情報保護法がその認定を受けるのは厳しいように思われる[27]。

(b)　国家の安全にかかわる法律との関係

さらに、***Schrems*** 事件は、テロなどの国家の安全や機密にかかわる制度（**security law, intelligence law**）の十分性を審査する必要性とその難しさを浮き彫りにした。いかなる国でも、その国の安全を守るためには、個人情報を強制的又は秘密裡に取得する手段を有しているともいわれている[28]。

よって、ＥＵがその市民のデータ保護を第三国でも貫徹しようとするのであれば、第三国のセキュリティ法が十分性を有するか否かについて、常に問題となるように思われる。だが、その具体的な十分性基準を示すことは容易でない。このことは、欧州委員会から十分性の決定を受けたプライバシー・シールドをみてもうかがい知る

ことができる。

(二)　組織に関する十分性（institutional adequacy）

十分性の審査は、以上のような実体的な保障内容に関する観点に加えて、その実体的な保障がいかなる執行制度、組織的体制によって確保されているか、という観点からも行われる。この点については、二つの問題がある。まずひとつ目は、監督機関の権限の範囲の問題である。ふたつ目は、独立した監督機関の必要性とその程度に関する問題である。

(a)　監督機関の権限の範囲

まず、ひとつ目の監督機関の権限の範囲について、ＧＤＰＲと改正個人情報保護法との対比において検討する。個人情報保護委員会には、欧州のデータ保護制度で重要視されてきた独立監督機関の立入検査（audit）（改正個人情報保護法四〇条）も認められるなど、その権限は近似してきているが、依然として、ＧＤＰＲで求められている独立監督機関の権限の範囲と日本のそれとは、重要な点で異なっている部分がある[29]。

たとえば、改正個人情報保護法では罰則の定めをおいているが（八二条以下）、ＧＤＰＲで認められているような個人情報保護委員会が制裁金を科すことはできない（ＧＤＰＲ五八条一(i)、八三条）。このＧＤＰＲの制裁金の仕組みは、刑事罰とは別の制度である。

日本では、現実的にも、理論的にも、ＧＤＰＲのように、場合によっては二〇〇〇万ユーロ（一ユーロ一二〇円で二四億円相当）又はそれを超え得る全世界年間売上高の四％という制裁金を科すことができる制度（八三条

五、六）を採用することは難しいのではないだろうか。

もっともこの制裁金制度を有しないEU加盟国もあり、その場合、GDPRではそれに代わる罰金制度で足りることを承認しているが（八三条九）、日本のような刑事罰制度のみで対応し、監督機関である個人情報保護委員会が制裁金を科す権限を有していない日本の制度が、この規定によってEUの十分性基準をクリアーできるのか明らかではない[30]。

(b) 監督機関の独立性

① 独立した監督機関の必要性

もうひとつは、「独立」監督機関の必要性とその程度に関する問題である。日本では、民間部門における個人情報の取扱い及び、公的部門における特定個人情報の取扱いを監視する独立した機関として、内閣府設置法四九条に基づき個人情報保護委員会が設置され、同委員会は独立して職権を行うこととされている（改正個人情報保護法六二条）。このように、同機関が独立性を確保したことについて反対するつもりは毛頭ない。しかし、個人情報保護の分野における独立した監視機関の必要性に関して十分な議論がなされたのかについては、若干の疑問がある。

日本では、欧州との関係で個人データ保護組織を比較して語るときに、区別されていないのではないかと感じられることがあるが、第三者機関を新たに設置することや既存の組織を利用することによって、「個人データ保護の所掌をひとつの部署に集めること」と「その機関が独立したものであること」とは別問題である。

個人データの取扱いが多くの分野に及ぶために、所掌事務を一元化することは望ましいというのはその通りで

あろうが、その事務を扱う行政機関が独立している必要があるというのはなぜなのだろうか。一般に、独立行政機関の設立は、当該分野の専門性や中立性[31]の見地から認められると解されている[32]。

個人データ保護の分野において専門的知見が必要であるということについては争いがないだろう。他方、中立性の要件は、個人情報保護の分野では、監督機関が公的部門を監督対象としている場合に、公平、公正な審査を行うために独立した監督機関が必要であると説明されている。つまり、監督対象となる公的機関からの介入（とりわけ上級機関からの指示や圧力など）を避けるために、監督機関の独立性を確保すべきであるというのである[33]。

とすれば、民間部門を監督する場合に、同様の理屈が通用するとは必ずしもいえないはずである。個人情報保護委員会は、いわゆるマイナンバー法に基づく、個人番号の取扱いについて監視、監督するものとされており、それ以外の個人情報の取扱い全般について公的部門を監督するものではない。よって、中立性の見地から同委員会が独立した機関でなければならないという説明とその監督対象との整合性が必ずしも図られているとはいえないように感じられるのである[34]。

もちろん、個人情報保護委員会は、当然、他の諸々の理由にも基づいて設けられた組織である。たとえば、個人情報の取扱いが複数の府省庁等の所轄分野にまたがる場合や主務大臣が明確でない場合があり、そうした場合にも、適切かつ迅速に対応できるようになるために設置されたものと説明されている[35]。つまり、主務大臣制の欠点を克服するものとして、同委員会が設立されたということである。しかし、この理由は、所掌事務を一か所に集中させるべき理由になったとしても、内閣の指揮監督から独立した機関が必要であるという根拠としては弱いように思われる。

結局、EUを中心とした国々でコミッショナー制度が採用されているということが、独立行政機関として、個

人情報保護委員会を設置する理由なのかもしれない。[36] しかし、そうであるとするならば、実体的な個人データ保護を図るために、ＥＵの執行機関と同様の制度が必要であるというのは理論的ではないように思われる。

というのも、実体的なデータ保護を確保する方法は、必ずしも、独立した監督機関によって実現されなければならないとはいえないからである。仮にこうした機関を欠いていたとしても、調整機関又は権限が集中した機関を有する行政組織制度、司法救済制度、また場合によっては、遵法精神の高い国民性の存在などによって、その実現が可能である。[40]

この点に関して、データ保護指令のもとでは、第三国に独立した監視機関の設置を十分性審査で要求いなかった―日本では、十分性審査で、そうした機関の設置が求められているという趣旨の論調が多く見受けられたが―ことに注意を要する。同指令の十分性審査の判断要素を明確化した二九条作業部会の文書（七頁(ii)）では、欧州では、独立行政機関という制度になじみがあるが、他の地域では、そうした制度になじみのない国も多くあることを認め、第三国における様々な司法手続やそれ以外の手続を考慮に入れて十分性を判断すると明示していたのである。[41]

にもかかわらず、監視機関における独立性の要件は、欧州でも日本でも、独り歩きをし始めることになる。そして、遂に、ＧＤＰＲでは、加盟国のみならず、第三国の十分性審査でもこの独立性要件を求めることとしたのである。これは、日本などの第三国が、この点に関するデータ保護指令を正確に理解し、ＥＵを説得してこなかったことにも責任の一端があるように感じられる。

もっとも、私見では以上の点について、もっぱら独立行政機関をいかなる要件のもとに設置するのかという理論的な関心から指摘したにとどまり、個人情報保護委員会が独立した監督機関として設置された以上、これを有

効に機能させない手はないと考えている。その意味で、今後、同委員会に公的部門全般に対する監督権限を付与する―むしろ、同委員会の独立性確保が強く要請されるのは、公的部門の個人情報取扱いの監視に実効性をもたせるためであるのだから―ことが、個人データ保護の包括的実効性を確保するためには必要となってこよう[37]。過去の多くの独立行政委員会のように、その活動が停滞し、実効性を失うようなものにならないことを期待したい。

② 独立性の程度

仮に、EUが独立した監督機関の設置を第三国に求めることが妥当だとしても、その機関が、EUの加盟国の個人データ保護機関に対して求められる独立性と同程度のものが十分性審査において要求されるのかについては、必ずしも明らかではない。

つまり、EUにおいても、その独立性の意味は自明ではないのである[38]。具体的には、データ保護指令二八条一項後段の「完全な独立性」（complete independence）の意味が争われており、これまでに、ドイツの州レベルのデータ保護監督機関やオーストリアのそれが、欧州司法裁判所の判決において、その独立性を否定されている[39]。

ドイツのケースでは、ドイツ政府が、右文言を機能的な独立性（functional independence）で足りると解釈し、州が行う州のデータ保護機関に対する調査は独立性を害するものではないと主張したのに対し、欧州委員会はあらゆる影響から自由でなければならないという、まさに文字通り完全な独立性を有しなければならないと主張し、この欧州委員会の主張が欧州司法裁判所で認められた。

仮に、第三国に求める独立監督機関の独立性の意味が、EU域内で求められている意味と同じであるとすれば、十分性の審査対象となる第三国の監督機関について、これらの判例やGDPRの条文と照らし合わせた検討が必

要となってこよう。また、この要件の意味がＥＵにおいても変化し続ける可能性がある以上、十分性認定を受けた第三国であっても、コンスタントにＥＵの独立性の要件との整合性について検証し続けなければならないことになろう。

㈢　欧州委員会による審査権行使の限界

ＥＵデータ保護規則では、欧州委員会が十分性審査を行うことが明示され、その審査対象としては、第三国、第三国における特定の分野や地域、国際機関であることが定められている。この部分については、これまでも、第三国、国家とは認められていない地域、カナダの営利組織のように特定の分野、セーフ・ハーバー協定に対して、十分性審査が行われてきたことに鑑みると、国際機関が加えられたことを除けば、必ずしもその審査対象が増加したとはいい切れない。

もともと、第三国の法体系や言語の異なる国々の制度を精査することは容易なことではなく、欧州委員会や加盟国のデータ保護機関の負担は相当なものであるが、その負担は、次の理由からさらに増加していくものと思われる。

① ***Schrems*** 判決を受けて、ＧＤＰＲでは、欧州委員会が十分性決定を受けた第三国のその後の展開を監視し続けること、また、少なくとも四年ごとに定期的な見直しを行うべきであると定められた（四五条三、四）。

② 欧州委員会の十分性決定に疑義があるにもかかわらず、個人データの第三国移転が行われている場合、加盟国における各データ保護機関は、その調査権限を行使しなければならない（***Schrems*** 判決）。

③ ＧＤＰＲでは、個人データを再移転する場合に、当該第三国や機関のデータ保護水準を審査対象とすること

が明示された（四五条二（ａ））。

①については、十分性決定を受けた国が増加するにつれて、欧州委員会の負担が恒常的に増大することになる。また、②については、各データ保護機関の負担が少なくないのみならず、それぞれの機関の調査が重複する（duplicative）おそれがある。

さらに、③については、移転先の監督機関の判断を信頼し、それに依拠するのではなく、ＥＵがその再移転先の第三国や機関のデータ保護水準を直接に調査するという意味であれば、世界中の個人データ保護状況を監督・監視し続けなければならないことになりかねず、相当な負担となる。

このように、第三国に対する十分性審査に関して、欧州委員会及び各監督機関は、向後、膨大な時間、労力、費用を負担し続けなければならない[42]。その結果得られるものが、その負担に見合うものであるのか、または、そうではなく、過度な官僚主義（bureaucratic）に陥っているにすぎないのかについては、検討する時期に来ているように思われるのである。

三　ＥＵ個人データ保護帝国主義からの離脱

㈠　ＥＵ基本権憲章の桎梏

ＥＵ基本権憲章は、二〇〇〇年に締結されたが、当初は法的拘束力を伴わないものであった。しかし、リスボン条約が二〇〇九年に発効したことに伴い、法的拘束力を有するようになった。同憲章の七条は、私的な又は家族の生活の尊重について、また、八条一項及び二項は、個人データの保護について定めている。さらに、八条三

項は、独立した監督機関の設置の必要性について定めている。

同憲章に法的拘束力が認められるようになった後に出された、欧州司法裁判所の *Google Spain* 判決、*Digital Rights Ireland* 判決[43]、*Schrems* 判決などでは、同憲章七条及び八条における権利の保護の重要性について繰り返し指摘している。とりわけ、欧州司法裁判所が、*Schrems* 判決において、個人データがＥＥＡ域内で移転される場合のみならず、第三国へ移転される場合においても、この憲章の重要性を指摘したことについては、大きな意味があるだろう。越境的個人データの移転についても、ＥＵ基本権憲章が適用されることが明らかとされたからである。

Schrems 判決では、第三国のデータ法制が十分性を充足すると判断するためには、その制度がＥＵの制度と同一のものである必要はないが（not identical）、同等のものである（equivalent）必要があるとし、その際に、同憲章におけるＥＵ市民の権利が侵害されることがあってはならないと判示した。しかし、そうなると、ＥＵ制度と同等のものという意味は、相当厳格に判断されることになるように思われる。また、「identical」と「equivalent」という概念に差があるとしても、その差は極めて不透明である。このように、基本権憲章が法的拘束力を有した結果、ＥＵの第三国に対して求める保護水準がさらに厳しくなることが予想される。

しかも、ＥＵは、基本的に公的部門及び民間部門の双方、つまり、個人データ保護制度全般についての十分性審査を想定しているが、とりわけ、公的部門でＥＵと同様の法制度を求めることは、相当程度無理があろう。このようなＥＵの要求に応えることができる国は少なく、ＥＵは自分で自分の首を絞めるような状況を作り出しているのである。

既に指摘したように、十分性を受けた国や地域の数は極めて少なく、さらに、ＥＵは、近年、その大きな貿易

相手国となっている中国の個人データ法制に対しては十分性審査を行っていない。さらに、EU域内の会社の多くは、個人データの処理をインドやパキスタンなどの企業に委託しているといわれているが、EUはこれらの国家の個人データ法制に対しても十分性審査を行っていない。EU基本権憲章の適用によって、こうした国々が十分性審査をクリアーする可能性はますます低くなったように思われるのである。

結局、EUは、BCRsやSCCsなど他の代替手段を広く提供し、これを充実させざるを得なくなっており(44)、現実には、B to Bの個人データのやり取りは、こちらの利用が一般的なものとなっている。もっとも、これらの代替手段が基本権憲章の権利を侵害するものであるか否かについては、注視していく必要があるだろう。

㈡　日本のこれまでの対応

日本を含む第三国は、これまで、EUのデータ保護法は、世界の最先端であり、これに比して日本は遅れていると考える傾向があったように思われる。EU自身もそう考えてきた節がある。確かに、EUデータ保護法制に学ぶところは多くあったし、現在でも多く存在する。このような考えは、日本において個人情報保護法制を創設し、整備する促進剤のような役割を果たしてきた(45)。

しかし、EUの十分性審査という点については、冷静に考えてみると、他国の法事情を鑑みずに、EUが事実上同様の法制度を求めていること自体おかしなことではないだろうか。EUの十分性審査は、個人データの越境移転における特定の法規定の制定を求めるというものにとどまるものではなく、個人データ保護に関する制度全般をEU水準にあることを求めるものであり、特異であるように思われる。恐らく、他の法領域において、このような押し付けが成功した例はあまりないのではないかと思う。

ＥＵが自らと同様の法制度を第三国に作り上げるように要求しているというメッセージは、ＥＵがそもそも描いていた構想であるのか、それとも、第三国が勘違いしＥＵを徐々にその気にさせた結果生じたものであるのかについて、判断することが難しい。ただ、次の点は指摘できよう。

ＥＵ個人データ保護指令が制定された当初は、ＥＵは、牧歌的に、ＥＥＡの域外にデータ移転するのであれば、適切な保護がなされた国へ移転して欲しいと考えていたに過ぎなかったが、データ移転を取り巻く環境が急激に変化していく過程も相俟って、日本を含めた第三国が過剰に反応していったという過程があるのではないかということである(46)。

また、個人データという分野に限ったことではないが、欧米から見た第三国には、欧米に対する懐疑的態度が欠如した西洋偏重主義ともいうべき国際派が存在する。また、非国際派の中には、語学ができるというだけで思考を遮断し、そのような国際派を評価する者がいる。こうした者の行動が、徐々にＥＵが持ち上げられていくことへの少なくとも遠因となったのではないかと思われるのである。

たとえば、日本では、越境的データ移転の代替手段として、同意、BCRs、SCCs 及び二国間協定といったものの有用性や実用性を検証することよりも、欧州の十分性評価を受けることが正しい途であるかのごとく主張されることが多かった。これらの代替手段は、真に利用できないものであったのか、また、アメリカ合衆国のように、セーフ・ハーバーやプライバシー・シールドのような協定を締結する選択肢は本当になかったのかという点について、十分に検討してきたとは言えないように思われるのである。

以上のような事情が重なり、十分性評価を受けることを第一義的に考える風潮が作り出され、ＥＵ個人データ保護帝国主義（EU Personal Data Protection Imperialism）ともいえるような状況を作り上げてしまう結果を生み

出してしまったのではないだろうか。

ともあれ、仮に、日本がＥＵの十分性評価を望む場合、個人情報保護委員会は、公的部門全般を監督・監視する権限を有しないため、民間部門に限ってその審査を受けることになろう。公的部門については、いわゆるマイナンバー法の範囲で十分性審査を受けることも理論的には考えられるが、この法に関連してＥＥＡ域内の個人データを日本に移転する必要性のある機会は想定しにくく、実益はほぼないのではなかろうか。

㈢　日本のとるべき途

個人データの移転が国境を超えて頻繁に行われている今日では、この点に焦点を当てた個人データ保護の取組みはもちろん大切なことである。しかし、少なくとも現段階において、日本がＥＵの十分性審査を受けるということに固執する必要は無いように思われる。むしろ、日本にとって必要かつ有益な制度を粛々と作り上げていくことが大切であろう。日本をはじめとする第三国が、こうしたＥＵの戦略にどこまで付き合うかは見極めが必要な時期に来ているように思われるのである。

もっとも、私見では、日本がＥＵの十分性審査を受けるべきでないと主張しているわけではない。この審査を受け、十分性ありと決定されれば、ＥＵとの個人データ移転に関する障壁は崩されることになり、日本にとって歓迎すべきことであろう。だが、日本が十分性審査を受けるという方針を採ったとしても、ＥＵが十分性審査の水準や判断方法を変化させない限り、その実現は困難であろう。

また、そもそもＥＵが第三国に十分性審査を受けてもらうという方針を貫くことには無理があるように思われる。個人データ保護の分野でもその保障内容、方法に文化の違いのあることが明らかとなりつつあるにもかかわ

らず、多くの国で同じような法律が採用されるよって、公的部門及び民間部門において例外なく――しかも、日本で公的部門といった場合独立行政法人等や地方公共団体の個人情報の取扱いも含まれることになる――規律、執行されるというのは理想論に近い。EUも、ここまでの構想を抱いていないのではないのではなかろうか。

そこで、EUのスタンスへの対処方針としては、次のようなアプローチが考えられる。公的部門についてみた場合、個人データが民間から政府へ越境的に移転される場合（B to G の移転）と、政府間で越境的に移転される場合（G to G の移転）とがあるが、EEAから類型的に個人データの移転が必要とされる場面は、民間部門に比して恐らく著しく少なく、その必要に迫られた場合には、政府間において、条約や行政取決めのなされることによって、個人データの保護は図られるように思われる。

また、民間部門についてみた場合、この取組みのアプローチとしては、それを国家レベルで、EUなどと協調した法制度の仕組みを政府自らが作り上げていくというものと、民間レベルで、その保護を図ろうとする企業や団体を募り自主的取組みを拡充していくというものがあり、それらのアプローチは、むろん、両立するものである。

しかし、前者のアプローチについては、越境的個人データの移転に関する問題を契機として、EUと同等の法的規制の網を企業や団体全体にかぶせること、すなわち、この民間部分全体でEUの十分性審査に見合う制度を作ることが必要かについては検討の余地がある。というのも、民間部門において、EEAからのデータ移転を必要とする団体は全体の何割程度であるか不明であるが、EUの十分性審査を目指すということは、EUからのデータ移転が全くない組織や団体に対しても、EUと同様の法制度による規制を課すということになるからである。これは、果たして妥当な価値判断だろうか。

利用者及び消費者としての一般人からすれば、民間団体間における越境的な個人データ移転（B to Bの移転）においては、その実質的保護を図っている民間企業や団体が容易に認識できれば良く、この点で、プライバシー・マーク制度などを利用した民間レベルの取組みの意義は、誠に大きいように思われる（GDPR四二条、四六条二(f)、改正個人情報保護法第四章第四節参照[47]）。

問題は、国際的に通用する信頼に足るマーク制度のようなものを民間中心に世界全体で作れるか否かにかかっており、その実現に向けた支援を政府はしていくべきであろう[48]。第三国がEUの満足する個人データ保護制度を整え、十分性審査を受けるという選択よりも、こちらの方が現実的かつ実効的なアプローチであるように思われる。

なお、こうした民間における取組みでは、強制的な執行の点において問題があるという指摘が良くなされる。しかし、個人データの保護を怠った企業や団体に対する最たる制裁は、消費者や利用者が離れることであろう。そのため、データ保護違反の事実を詳細に公開することや保護団体であるという認定を取り消すことなどによって、十分その取組みの実効性を確保できる――できないというのであれば、たとえば、BCRsやプライバシー・シールドのように、執行面を国が担保するほかない――ように思われる。

さらに、こうした制度のもとでも、*Schrems*判決で争点になったように、国家の安全にかかわるという理由で個人データが収集される公権力の行使を忌避することができないという問題が残存する。この場合に、データ監督機関が第三国の国家の安全にかかわる立法をすべて調査するというのは、不可能ではないにせよ、大変な労力を伴うことである。

そこで、この範囲においては、移転先の国家安全に関する法に従うというデータ主体の同意をもって足りると

解すべきである。つまり、第三国に個人データ保護に関する適切な一般的仕組みを作り上げてもらうことは重要であるが、その仕組みの枠を超える安全保障にかかわるようなデータ収集については、その第三国からのサービス提供・利用を求める利用者や消費者からの同意をもって足りると考えるのである（第三国国民と同一条件の原則）。

つい最近まで、個人データ保護を研究する日本人の専門家は、EUが一枚岩だと信じてきた者が少なからずいる。しかし、イギリスは、二〇一六年六月にEUからの離脱を国民投票で決めた。ドイツの一人勝ちといわれるEUで離脱ドミノがこれから起きないという保証はない。イギリスが、今後、経済的な成功をおさめるようなことがあれば、それは十分現実味を帯びてくる。

その場合にも、日本は、EUに固執するのかという点を含め、今一度、EUの第三国に対するデータ保護体制を冷静に見極める時が来ているのではないだろうか。法制度を策定するときに、政治的、外交的、経済的要因などがつきものであるにせよ、自国の個人データ保護にとって、真に資するものであるのかという視点に立ち返ることが必要とされているのかもしれない。

注

＊本稿は、主に、前アイルランドデータ保護コミッショナーのビリー・ホークス氏との議論、また、私が二〇一五年に担当したトリニティ・カレッジ・ダブリン大学大学院の「プライバシーとデータ保護」と称する講義の受講学生との議論において、考えたところをまとめたものである。これらの方々に御礼申し上げたい。また、亜細亜大学の海外研究制度によっ

て、二〇一五年四月から一年間、研究に専念するという貴重な機会が与えられたことについても、普段の恵まれた研究環境を与えられていることと合わせて、感謝したい。本稿が、亜細亜大学法学部五〇周年という節目の号に掲載されることも、大変うれしく思う。

（1）COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century.

（2）Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

（3）これらの提案の詳しい経緯や内容については、石井夏生利『個人情報保護法の現在と未来』（勁草書房、二〇一四年）四三－一七〇頁を参照。

（4）Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

本規則の仮訳については、一般財団法人日本情報経済社会推進協会（JIPDEC）のホームページで公表されている（https://www.jipdec.or.jp/library/archives/gdpr.html）。なお、この翻訳は、厳しい時間的な制約を伴う中で作られた仮訳であり（もとより、外国法の翻訳が完訳となることは困難を極めるが）、かつ、リサイタルの部分を欠いたものであるが、今後、適宜、追加及び修正が加えられることが期待される。

（5）Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA; Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

（6）同作業部会は、文字通り、データ保護指令二九条のもとに設置された機関である。同機関は、諮問的なものであるが、独立してその職権を行使する。この機関は、GDPRにおいて、その地位がさらに高められ、欧州データ保護会議（European Data Protection Board）に改組された（六八条～七六条）。

（7）'Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' adopted on 24 July 1998.

（8）*Maximillian Schrems v. Data Protection Commissioner* (C-362/14) [2015].

（9）Christopher Kuner, 'Developing an Adequate Legal Framework for International Data Transfers' in Serge Gutwirth et al. (eds), *Reinventing Data Protection?* (Springer 2009) 263, 266-267.

（10）http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

（11）アルゼンチンの十分性が、究極的には政治的な理由で認められたと Kuner 氏は指摘している（Kuner, 'Developing an Adequate Legal Framework for International Data Transfers', 265, 271）。

（12）二九条作業部会は、二〇〇一年一月に、オーストラリアに対する十分性審査の第一次審査として、同国の個人情報保護制度が十分性を満たすものではないと判断した（Article 29 Data Protection Working Party Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, adopted on 26 January 2001(WP40)）。この結果を受けて、オーストラリアは、当該法制度を改正したが、その後、十分性審査を受けてパスしたという情報はこれまでのところない。この経緯については、石井九〇－九一頁を参照。

（13）'Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce' Decision 2000/520/EC.

（14）この frivolous and vexatious という言葉は、法的な根拠が薄弱であるというような、もちろん法的な意味で使われているが、この言葉の持つネガティヴかつインパクトのある語感のためであろうか、新聞報道、専門家のコメント、文献などで頻繁に引用された。それは、アイルランドのデータ保護コミッショナーが、データ保護に消極的であるかのような印象を与えることに役立った（その後、アイルランドデータ保護機関の大幅な人員及び予算の増加につな

がったため、プラスの面もある）。しかし、Schrems 氏は、そのほかにも多くの苦情申し立てをしており、それらのすべてについて、同コミッショナーが専門家を雇い調査を行っていた。その結果を Schrems 氏に報告する予定であった矢先、セーフ・ハーバーに関する苦情に的を絞り、これについて提訴するため、それ以外の申し立てを取り下げたのである。

（15）*Maximiliam Schrems v. Data Protection Commissioner* [2014] IEHC 310.

（16）一部で誤解があるように思われるが、欧州司法裁判所は、セーフ・ハーバーについて無効と判断したのではなく、同制度の十分性を認めた欧州委員会の決定を無効と判断したのである。事実上、セーフ・ハーバー協定を無効としたともいい得るが、欧州司法裁判所は、同協定に十分性の決定を与えた欧州委員会の判断によって、ＥＵ市民の権利が侵害されていること、また、同委員会がそれを認識していたことなどを理由に、同決定を無効と判示したのである。

（17）この判決に対する日本の評釈としては、次のようなものがある。

藤井秀之「欧州司法裁判所によるセーフハーバー協定無効判決について」InfoCom ニューズレター（情報通信総合研究所、二〇一五年）（https://www.icr.co.jp/newsletter/law20151008-fujii.html）。

フレデリック・ルイ、杉本武重、イツィック・ベニズリ「欧州委員会のセーフハーバー決定を無効とした欧州連合司法裁判所二〇一五年一〇月六日付判決」国際商事法務第四三巻一一号（二〇一五年）一七五〇頁。

中西優美子「ＥＵから第三国への個人データ移転と欧州委員会のセーフ・ハーバー決定（Ⅵ㈣）自治研究第九二巻第九号（二〇一六年）九六頁。

中村民雄「フェイスブック個人情報域外移転事件」法律時報八八巻八号（二〇一六年）一一二頁。

拙稿「Implications of the Judgement on the US Safe Harbour Agreement」比較法雑誌五〇巻四号（二〇一七年）（脱稿済み）。

（18）プライバシー・シールドは、複数のアメリカ合衆国の官庁から出された多くの文書からなる。この全体のリストについては、商務省から欧州委員会への文書で示されている（http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-1_en.pdf）。また、その具体的な内容については、次のサイトから入手可能である（http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf）。

(19) 'COMMISSION IMPLEMENTING DECISION of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield' C(2016) 4176 final.

(20) 'Statement of the Article 29 Working Party' issued on 16 October 2015.

(21) アイルランドのデータ保護コミッショナーのホームページに、この経緯が記されている（'Update on Litigation Involving Facebook and Maximilian Schrems' https://www.dataprotection.ie/docs/28-9-2016-Explanatory-memo-on-litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm）。

(22) 'Opinion 15/2011 on the definition of consent' adopted on 13 July 2011.

(23) 越境的個人データの移転に限らず、同意を個人データ移転の法的基礎とすることの問題性については、既に多くの専門家によって指摘されている（see e.g. Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880; Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (Fall 2011) 140 Dœdalus, Journal of the American Academy of Arts & Sciences 32）。その同意に対する批判の骨子は、インフォームド・コンセント（informed consent）の実現困難性、及び、同意と引き換えに受ける利益との不均衡（disproportionate trade-off）とにまとめることができるように思われる。

(24) *Google Spain SL and Google Inc. v. Agencia Espanola de Protection de Datos* (C-131/12) [2014].

(25) 行政手続における特定の個人を識別するための番号の利用等に関する法律（いわゆるマイナンバー法）二九条の四では、特定個人情報の漏えいなどが生じた場合、個人番号利用事務等実施者が個人情報保護委員会へ報告することを求めている。

(26) 藤原靜雄「個人情報保護に関する国際的ハーモナイゼーション」論究ジュリスト一八号（有斐閣、二〇一六年）六四、六六－六八頁。

(27) 結論同旨、宮下紘『事例で学ぶプライバシー』（朝陽会、二〇一六年）一三二頁。

(28) 欧州人権裁判所（European Court of Human Rights）では、国家の安全を理由とした包括的かつ無差別的な個人データの収集について、ハンガリーとロシアのケースが争われ、いずれのケースでも、当該法律の違法性を認めた（*Szabo*

and Vissy v. Hungary App No 37138/14 (12 January 2016); *Roman Zakharov v. Russia* App No 47143/06 (4 December 2015))。

(29) 日本の独立監督機関である個人情報保護委員会の権限については、日置巴美・板倉陽一郎『平成二七年改正個人情報保護法のしくみ』（商事法務、二〇一五年）五八－五九頁の表が詳しい。

(30) 日本のデータ保護機関に課徴金（制裁金）を課す権限を与えるよう検討すべきであると主張する論稿として、二関辰郎「第三者機関を通じたパーソナルデータの保護」自由と正義六五巻一二号（二〇一四年）三二、三八頁、宍戸常寿「個人情報保護委員会」ジュリスト一四八九号（二〇一六年）四二、四八頁がある。

(31) この専門性や中立性という意味が明確性を欠いていることを指摘するものとして、黒川伸一「職権行使の独立と立法機能の限界」法学新報一二〇巻第一・二号（二〇一三年）一二三、一二六－一三〇頁を参照。黒川教授は、専門性から独立行政機関を設けるべきと演繹されるかについては、検討の余地があると主張しているが、同感である。

(32) アメリカ合衆国における独立行政機関の正当化論拠やその合憲性に関して検討を加えた労作として、駒村圭吾『権力分立の諸相』（南窓社、一九九九年）がある。そこで、駒村教授は、政治的中立性・専門性に替えた新たな論拠として、政府の失敗（誠実執行の挫折）、熟慮的討議等が据えられるべきであるとしている（なお、同「内閣の行政権と行政委員会」憲法の争点（有斐閣、二〇〇八年）二二八頁も参照）。

(33) 個人データに限ったことではないが、公的部門によるデータ収集やその利用に対する監視という観点からすれば、そのデータをいかに公に開示するかという情報公開の点においても、独立した第三者機関によって公権力を監視する必要性が高い（むしろこちらの方がその必要性が高いとも考えられる）ように思われる。

この問題は、とりわけ、国家秘密の公開を巡って顕在化するが、その司法的統制を論じたものとして、寒河江和樹「政府による情報秘匿と情報公開訴訟―国家秘密に対する司法審査の意義と限界―」法学新報一二三巻第三・四号（二〇一六年）一三一頁を参照。寒河江氏の指摘するように、この分野における司法的統制が必ずしも容易でないという現実があるのであれば、独立した第三者機関の設立はその解決の一助となり得るだろう。

(34) 宍戸教授も、同様の趣旨から、特定個人情報保護委員会と個人情報保護委員会とは質的相違があると指摘している（宍戸常寿「パーソナルデータに関する「独立第三者機関」について」ジュリスト一四六四号（二〇一四年）一八頁、

二一頁）。

（35）日置『平成二七年改正個人情報保護法のしくみ』五一頁。

（36）宍戸「パーソナルデータに関する「独立第三者機関」について」一九頁。個人情報保護委員会を独立した第三者機関として設置した経緯や説明については、この宍戸教授の論稿がまとまっており参考になった。なお、宍戸教授は、安全に関わる個人情報は、その取扱いが政府内部で不透明な形で完結することが懸念されるという意味で独立した監視機関の存在が構造的要請と考えられるという（「安全・安心とプライバシー」論究ジュリスト一八号（二〇一六年夏号、有斐閣）五四、五九頁）。だが、本文で指摘したように日本の個人情報保護委員会の監視対象が民間部門とマイナンバー法での個人情報の取扱いであることに鑑みると、少なくとも、同委員会が独立した機関であるべきことの説明とはならないように思われる（ただし、宍戸教授が、同委員会の独立性の根拠として挙げているのではないようにも読める）。

（37）同旨、新保史生「改正個人情報保護法の論点」憲法研究第四八号（二〇一六年）四六－四八頁。

（38）アメリカ合衆国における独立機関の「独立」の意義のとらえ方が、その機関の正当化根拠をいかに捉えるかによって異なることを明らかにした研究として、駒村『権力分立の諸相』第二章を参照。

（39）*European Commission v. Federal Republic of Germany* (C-518/07) [2010]; *European Commission v. Republic of Austria* (C-614/10) [2012].

（40）ＥＵ諸国でもそのような判断が実際にはなされているようであるという指摘として、藤原靜雄「公的部門の個人情報保護法制の見直し」法律時報八八巻一号（二〇一六年）七四、七八頁を参照。

（41）注（7）を参照。

（42）Kuner 氏は、十分性審査をＥＵが維持し続けることに否定的であり、それに代わって、第三国へとデータ移転するものに責任を課すというアカウンタビリティ（accountability）に力点を置くべきであると主張している（Developing an Adequate Legal Framework for International Data Transfers', 269-272）。

（43）*Digital Rights Ireland and Others* (C-293/12 and C-594/12) [2014].

（44）Lynskey 教授は、ＧＤＰＲでは、十分性審査を中核に据えることから、BCRs の利用方法を規定に盛り込むなど他

の手段によるデータ移転にシフトしていると評価している（Orla Lynskey, 'The Foundations of EU Data Protection Law' (Oxford University Press 2015) 44）。

（45）本稿で改めて指摘するまでもないことであるが、この点に鑑みると、いち早く諸外国の状況を日本に伝え、個人情報保護制度の整備を推進してきた現個人情報保護委員会委員長である堀部政男先生の功績は極めて大きい。

（46）同旨、Orla Lynskey, 'The Foundations of EU Data Protection Law' 41-44 を参照。

Lynskey 教授は、ＥＵデータ保護指令制度を成り行きの優位性（supremacy by default）と称し、第三国に対するＥＵルールの優位性の確立は付随的、偶発的に生まれた結果（incidental effect）であり、第三国はＥＵへの制度の承認というよりも実利的観点からこれに従ったと主張している。他方、同教授は、ＧＤＰＲ制度を企図された優位性（supremacy by design）と称し、本規則が、ＥＵ在住のデータ主体に対する商品又はサービスの提供やそれらの者の行動監視を行う場合、ＥＵ域内に拠点のない管理者又は取扱者によるＥＵ在住のデータ主体の個人データの取扱いにも適用されるという点では（三条(2)を参照）、ＥＵがその市民の権利を守るため、同規則の優位性を他国においても図ろうとしていると指摘している（四四頁）。

（47）Kuner 氏は、民間によるイニシャティヴとして、BCRs、SCCs、セーフ・ハーバーなどをあげている（Kuner, 'Transborder Data Flows and Data Privacy Law' (Oxford University Press 2013) 92-96）。これらの制度は、データ保護監督機関を中心とした公的機関が、とりわけ執行面を担保するという形で関与するという点で、ＰマークやＪＩＳ規格のような民間の取組みと区別されるが、両者は、この制度の利用を望む団体や企業のみが自発的に利用するという点で共通している。

（48）このような観点から、ＡＰＥＣにおけるＣＢＰＲ（Cross Border Privacy Rules、ＡＰＥＣ越境プライバシールール）の取組みは、注目に値しよう。